$$M' \equiv C^{d} (\mathrm{mod}\ n)$$

where d is a multiplicative inverse of e(mod(1 cm((p − 1),(q − 1)))).

**2**. A system according to claim **1** wherein at least one of said transforming means comprises:

a first register means for receiving and storing a first digital signal representative of said signal-to-be-transformed,

a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,

a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

**3**. A communications system for transferring message signals $M_i$, comprising k terminals, wherein each terminal is characterized by an encoding key $E_i=(e_i, n_i)$ and decoding key $D_i=(e_i, n_i)$, where i=1,2, . . . ,k, and wherein

Mi corrresponds to a number representative of a message signal to be transmitted from the $i^{th}$ terminal, and

$$0 \leqq M_i \leqq n_i - 1,$$

$n_i$ is a composite number of the form

$$n_i = p_i \cdot q_i$$

$p_i$ and $q_i$ are prime numbers,

$e_i$ is relatively prime to 1 cm(p − 1,q − 1),

$d_i$ is a multiplicative inverse of

$$e_i(\mathrm{mod}(1\ \mathrm{cm}((p_i - 1), (q_i - 1))))$$

wherein a first terminal includes means for encoding a digital message word signal $M_a$ for transmission from said first terminal (i=A) to a second terminal (i=B), said first terminal including:

means for transforming said message word signal $M_A$ to a signed message word signal $M_{As}$, $M_{As}$ corresponding to a number representative of an encoded form of said message word signal $M_A$, whereby:

$$M_{As} \equiv M_A^{dA} (\mathrm{mod}\ n_A).$$

**4**. A system according to claim **3** wherein at least one of said transforming means comprises:

a first register means for receiving and storing a first digital signal representative of said signal-to-be-transformed,

a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,

a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying muliplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

**5**. The system of claim **3** further comprising:

means for transmitting said signal message word signal $M_{As}$ from said first terminal to said second terminal, and

wherein said second terminal includes means for decoding said signed message word signal $M_{As}$ to said message word signal $M_A$, said second terminal including:

means for transforming said ciphertext word signal $C_A$ to said message word signal $M_A$, whereby

$$M_A \equiv M_{As}^{eA} (\mathrm{mod}\ n_A).$$

**6**. The system of claim **3** wherein said encoding means further comprises: